THAT WHICH IS CLAIMED IS:

1. A method of authenticating a message from a client using a first authentication protocol to a resource manager using a second authentication protocol different from the first authentication protocol, the method comprising:

generating a second message from the message from the client, the second message including information from the client which has been authenticated using the first authentication protocol;

authenticating the second message using the second authentication protocol; and

providing the authenticated second message to the resource manager.

2. The method of Claim 1, wherein the first authentication protocol comprises Kerberos and the second authentication protocol comprises public key infrastructure (PKI).

3. The method of Claim 2, wherein the step of authenticating the second message comprises signing the second message with a private key corresponding to a PKI certificate available to the resource manager so as to provide the second message with a signature.

4. The method of Claim 3, wherein the step of generating a second message comprises:

receiving a Kerberos ticket;

verifying authenticity of the Kerberos ticket;

extracting principal information from the Kerberos ticket if the authenticity of the ticket is verified; and

generating the second message utilizing the extracted principal information.

5. The method of Claim 4, wherein the step of generating the second message utilizing the extracted principal information comprises incorporating the

principal information with data from the message from the client to provide the second message.

6. The method of Claim 5, wherein the resource manager carries out the steps of:

receiving the second message;

authenticating the signature of the second message;

extracting the principal information from the second message; and

processing the data from the second message based on the principal information from the second message if the signature of the second message is authentic.

7. The method of Claim 4, wherein the step of generating the second message utilizing the extracted principal information comprises generating at least a first component and a second component of the second message, the first component containing the principal information and the second component containing data from the message from the client.

8. The method of Claim 7, wherein the step of signing the second message with a private key comprises signing the first component with the private key and signing the second component with the private key.

9. The method of Claim 8, wherein the resource manager carries out the steps of:

receiving the at least two second messages;

authenticating the signatures of the second message;

extracting the principal information from the first component;

extracting the data from the second component; and

processing the data of the second component based on the principal information from the first component if the signatures of the at least two second messages are authentic.

10. The method of Claim 4, wherein the step of receiving a Kerberos ticket comprises receiving a Kerberos service ticket from a middle-tier server.

11. The method of Claim 10, wherein the step of providing the authenticated second message to the resource manager comprises returning the authenticated second message to the middle-tier server.

12. The method of Claim 11, wherein the Kerberos service ticket and the authenticated second message are encrypted.

13. The method of Claim 10, wherein the Kerberos service ticket is obtained by the middle-tier server responsive to receiving a delegatable Kerberos ticket.

14. The method of Claim 10 further comprising incorporating an identification of the middle-tier server in the second message.

15. A method of providing authentication for communications between a Kerberos client and a public key infrastructure (PKI) server, the method comprising:

authenticating a message from the Kerberos client at a party trusted by the PKI server;

signing the authenticated message with the PKI private key of the party trusted by the PKI server; and

forwarding the signed authenticated message to the PKI server.

16. The method of Claim 15, further comprising incorporating an identification of a principal of the message from the Kerberos client with the signed authenticated message.

17. The method of Claim 16, wherein the step of incorporating an identification of a principal of the message comprises incorporating the identification of the principal in the message from the Kerberos client.

18. The method of Claim 16, wherein the step of incorporating an identification of the principal of the message comprises incorporating the identification of the principal into a second message signed with the private key, and wherein forwarding the signed authenticated message comprises forwarding the signed authenticated message and the second message to the PKI server.

19. The method of Claim 15, wherein the step of authenticating the message is performed responsive to receiving a Kerberos service ticket.

20. The method of Claim 19, further comprising incorporating an identification of a source of the Kerberos service ticket with the signed authenticated message.

21. A system for authentication of messages from a client utilizing Kerberos authentication and a resource manager utilizing public key infrastructure (PKI) authentication, comprising:

a public key signature service configured to receive a Kerberos service ticket, authenticate the Kerberos service ticket, generate a message incorporating data associated with the authenticated Kerberos service ticket which is signed using a digital signature based on a PKI private key and PKI certificate so as to allow the resource manager to authenticate the message and provide the signed message to the resource manager.

22. The system of Claim 21, wherein the public key signature service is further configured to extract principal information from the Kerberos service ticket and incorporate the principal information with the message.

23. The system of Claim 21, further comprising a middle-tier server configured to obtain the Kerberos service ticket responsive to receipt of a delegatable Kerberos ticket and to provide the obtained Kerberos service ticket to the public key signature service.

24. The system of Claim 23, wherein the public key signature service is further configured to provide the signed message to the resource manager by returning the signed message to the middle-tier server and wherein the middle-tier server is further configured to forward the signed message returned by the public key signature service to the resource manager.

25. The system of Claim 24, wherein the public key signature service is further configured to extract middle-tier server information from the Kerberos service ticket and incorporate the middle-tier server information with the message.

26. The system of Claim 22, wherein the public key signature service is further configured to selectively incorporate the principal information into the message with the data associated with the Kerberos service ticket and to selectively generate a second message associated with the message containing the data associated with the Kerberos ticket which contains the principal information and sign the message containing the data and the second message if the second message is generated.

27. A system for authenticating a message from a client using a first authentication protocol and a resource manager using a second authentication protocol different from the first authentication protocol, comprising:

means for generating a second message from the message from the client, the second message including information from the client which has been authenticated using the first authentication protocol;

means for authenticating the second message using the second authentication protocol; and

means for providing the authenticated second message to the resource manager.

28. A system for providing authentication for communications between a Kerberos client and a public key infrastructure (PKI) server, comprising:

means for authenticating a message from the Kerberos client at a party trusted by the PKI server;

means for signing the authenticated message with the PKI private key of the party trusted by the PKI server; and

means for forwarding the signed authenticated message to the PKI server.

29. A computer program product for authenticating a message from a client using a first authentication protocol and a resource manager using a second authentication protocol different from the first authentication protocol, comprising:

a computer readable storage media having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which generates a second message from the message from the client, the second message including information from the client which has been authenticated using the first authentication protocol;

computer readable program code which authenticates the second message using the second authentication protocol; and

computer readable program code which provides the authenticated second message to the resource manager.

30. A computer program product for providing authentication for communications between a Kerberos client and a public key infrastructure (PKI) server, comprising:

a computer readable storage media having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which authenticates a message from the Kerberos client at a party trusted by the PKI server;

computer readable program code which signs the authenticated message with the PKI private key of the party trusted by the PKI server; and

computer readable program code which forwards the signed authenticated message to the PKI server.